POLÍTICA, CIÊNCIA E CRUELDADE
POLICY, SCIENCE, AND CRUELTY

SILVA JÚNIOR, Nelmon J.[1]

RESUMO: Reflexão sobre a quem servem os governos.
PALAVRAS-CHAVE: Cibercrime. Ciberterror. Cibermáfia. Ciência. Governo.

ABSTRACT: Reflection on the governments they serve.
KEYWORDS: Cybercrime. Ciberterror. Cibermáfia. Science. Government.

O presente artigo, inicialmente, foi elaborado a convite de revista científica vinculada a uma Universidade Federal nacional, para a qual o presente não foi satisfatório, vez que retrata cristalinamente a infeliz realidade jurídico-administrativa nacional, referente à política de segurança em relação aos crimes cibernéticos.

Ao falarmos algo sobre cibercrime, devemos anteriormente lembrar que este conceito foi utilizado pela primeira vez por Willian Gibson, em sua emblemática obra *Neuromancer* (1984). Mas afinal como conceituar cibercrime? Para melhor entendermos o tema, relembro a doutrina de Cédric Thévenet, quando leciona sobre ataques cibernéticos, que sob sua óptica, podem dar-se de três formas:

> Une attaque physique implique des armes conventionnelles dirigées contre des centres informatiques ou des ensembles de câbles assurant les liaisons; une attaque électronique implique l'utilisation de l'énergie électromagnétique comme une arme. C'est utiliser une impulsion électromagnétique pour surcharger les circuits des ordinateurs, ou, dans une forme moins violente, insérer un flux de code numérique malicieux dans les transmissions micro-onde de l'ennemi; e une attaque Informatique implique généralement l'utilisation de code malicieux comme arme pour infecter des ordinateurs en exploitant certaines failles logicielles.[2]

[1] **CIENTISTA E ESTUDIOSO DO DIREITO (PROCESSUAL) PENAL - CV Lattes:** http://lattes.cnpq.br/7382506870445908
1.MANTENEDOR DOS BLOGS CIENTÍFICOS:
http://ensaiosjuridicos.wordpress.com - http://propriedadeindustriallivre.wordpress.com
2. CIENTISTA COLABORADOR: Universidade Federal de Santa Catarina – UFSC (Portal de e-governo) http://www.egov.ufsc.br/portal/ - Glocal University Network http://www.glocaluniversitynetwork.eu/ (ITA)
3. MEMBRO: Centro de Estudios de Justicia de las Américas – CEJA (AL); Instituto de Criminologia e Política Criminal – ICPC; Associação Brasileira dos Advogados Criminalistas – ABRACRIM; Associação dos Advogados Criminalistas do Paraná – APACRIMI; International Criminal Law – ICL (EUA); National Association of Criminal Defense Lawyers (EUA).
4. MEMBRO FUNDADOR: Associação Industrial e Comercial de Fogos de Artifícios do Paraná/PR; e AINCOFAPAR (Conselheiro Jurídico), Associação Bragantina de Poetas e Escritores
5. COLABORADOR DAS SEGUINTES MÍDIAS: www.arcos.org.br - www.conteudojuridico.com.br - http://artigocientifico.uol.com.br - http://www.academia.edu/ - http://pt.scribd.com/ - http://www.academicoo.com/
6. AUTOR DOS SEGUINTES LIVROS CIENTÍFICOS: Fogos de Artifício e a Lei Penal; Coletâneas; e Propriedade Intelectual Livre.
7. AUTOR DOS SEGUINTES LIVROS LITERÁRIOS: Nofretete, Copo Trincado, e Valhala.

[2] THEVENET. Cédric., ***CYBER-TERRORISME, MYTHE OU REALITE ?***. Centre d'Etudes Scientifiques de Défense – CESD. 2005. Livro disponível em http://ensaiosjuridicos.files.wordpress.com/2013/06/50195426-2006-thevenet-cyberterrorism.pdf.

***Copyrigth* © 2013 - SILVA JR., Nelmon J.** (L. 10753/03 - OPL v.1.0 – FSF/GNU GPL/Key administrated by: CC BY-NC-ND, v.3.0)

Permito-me avançar, afirmando que entendo existirem quatro formas distintas de classificação dos criminosos cibernéticos: I) o criminoso eventual (no caso do jovem que comete determinado ilícito no mundo virtual motivado por sua repercussão em sua tribo ou grupo); II) o criminoso não eventual ligado a grupos organizados, objetivando benefício econômico próprio; III) igualmente de caráter não eventual, porém aqui o criminoso cumpre com seu objetivo que é determinado pelo grupo a qual serve (comum na cibermáfia); e IV) também possui caráter não eventual, mas aqui impera o objetivo político do grupo (segundo conceitos do ciberterrorismo e hactivismo).

Para PAGET, François., em *White paper, cibercrime e hacktivismo*, da McAfee Labs™ (2010)[3]:

> O termo *máfia* não deve ser empregado levianamente. Fora da Itália e não considerando a máfia russa, existem duas outras organizações criminosas que claramente se qualificam como *máfias*: as tríades chinesas e as yakuzas japonesas. Em todos esses grupos, é fácil identificar determinadas características:
> • A construção de mitos para justificar o crédito dado à imagem de "crime honorável".
> • Rituais e códigos.
> • Uma duplicidade legal/ilegal em relação às atividades realizadas.
> • Inegável intimidade com as mais altas esferas do poder.
> A eficácia das maiores forças criminosas decorre principalmente de sua hierarquia. Elas geralmente preservam um modelo de clã ou de família patriarcal; a submissão é o princípio e a hierarquia é a estrutura. Trata-se de um sistema implacável, onde não há lugar para personalidade entre os recrutas, os quais estão lá apenas para executar suas ordens com profissionalismo e unicamente em benefício da organização.
> Os recrutas não têm controle algum sobre o objetivo de suas ações, nem são consultados sobre elas. A violência reduz a resistência. Ela garante o silêncio pelo medo da retaliação.
> Os grupos criminosos são mais facilmente formados em sociedades problemáticas ou em períodos caóticos. Em troca de obediência, eles oferecem proteção individual. Os juramentos feitos por todos os membros das máfias tradicionais incluem uma obrigação de solidariedade e apoio à família em caso de prisão ou morte.

Delimitado (mesmo que sumariamente) o tema, relembro minhas ulteriores palavras em *Ciber terror & ciber guerra*: *"Duas verdades são inquestionáveis: a transnacionalização das leis; e eventual(is) ciberguerra(s) advinda(s) do ciberterrorismo. [...] O que seu País tem feito em relação a isto?"*[4]. Prossigo reafirmando:

> Dito isto, passo a desenvolver meu raciocínio, como faziam os socráticos, através da maiêutica[5]. 1. Nossos Oficiais das Forças Armadas, Parlamentares e Líderes do Executivo e Legislativo possuem conhecimento técnico-científico suficiente para bem atuarem no combate e prevenção ao cibercrime e ciberterrorismo? 2. Seria mais prudente, ao invés

---

3 Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/79513582-mcafee-cybercrime-hactivism.pdf.

4 Texto disponível em: http://ensaiosjuridicos.wordpress.com/2013/06/25/ciber-terror-ciber-guerra-nelmon-j-silva-jr/.

5 A maiêutica é um método de ensino socrático, no qual o professor se utiliza de perguntas que se multiplicam para levar o aluno a responder às próprias questões.

***Copyrigth* © 2013 - SILVA JR., Nelmon J.** (L. 10753/03 - OPL v.1.0 – FSF/GNU GPL/Key administrated by: CC BY-NC-ND, v.3.0)

de aprovar(em)-se lei(s) às pressas, convocar estudiosos e cientistas desta vasta e complexa matéria, para elaborarem um projeto de lei, definindo condutas delitivas e respectivas sanções legais? 3. Estratégias cibernéticas antiterroristas são necessárias ao reguardo da nossa Soberania? 4. Exemplos pedagógicos como os hodiernamente adotados pela Índia e China, devem ser priorizados pelo Governo Federal?[6]

Vou além, *"o Direito não serve ao modelo de governo duma Nação, mas sim ao seu sistema econômico, que em nosso tempo tende à transnacionalidade legal, por socialista*[7]*"*. Partindo dessa premissa, cito os exemplos adotados pela Índia e Estados Unidos da América, onde seus governos estabeleceram robustas políticas pedagógico-preventivas[8], que através do ambiente cibernético formam profissionais (normalmente de nível técnico, formação ofertada inclusive a estrangeiros) aptos – quando necessário – a atuarem no combate ao cibercrime.

Percebam que no Brasil a política quanto à segurança cibernética adotada - se é que existente - é diametralmente oposta àquelas, pois além de não serem adotadas estratégias similares, nosso governo deixa de utilizar o conhecimento de seus cientistas na solução de problemas advindos do espeço cibernético, como no recente episódio de espionagem praticada pelos Estados Unidos da América.

Lembro-me - com irônica graça - das notícias vinculadas naquela época, onde afirmou-se, por exemplo, que nosso governo buscaria junto à *International Telecomunications Union – ITU* subsídios para sua atuação no caso. Gizo que tais informações foram gratuitamente disponibilizadas em meu blog[9] (especialmente em *Research on legislation in data privacy, security and the prevention of cybercrime – UIT – 2006)*[10]. Infelizmente *"crueldades"* como esta aqui denunciada, tem sido freqüentes em países de modernidade tardia,[11] e somente hão de cessar quando nosso(s) governo(s) entender(em) a Quem Serve(m)!

---

[6] SILVA JÚNIOR, Nelmon J. ***ESPIONAGEM E FILOSOFIA***. 2013. Texto disponível em: http://ensaiosjuridicos.wordpress.com/2013/07/09/espionagem-filosofia-nelmon-j-silva-jr/.

[7] SILVA JÚNIOR, Nelmon J. ***PARÁDEIGMA.*** 2013. Texto disponível em: http://ensaiosjuridicos.wordpress.com/2013/10/04/paradeigma-silva-junior-nelmon-j/.

[8] Como exemplo cito os ambientes: *Cyber School of Law*, na Índia; e *Coursera*, nos EUA.

[9] À exemplo, posso citar os seguintes livros:http://ensaiosjuridicos.files.wordpress.com/2013/06/d-ind-ictoi-2011-sum-pdf-s.pdf - http://ensaiosjuridicos.files.wordpress.com/2013/06/d-ind-ictoi-2012-sum-pdf-s.pdf - http://ensaiosjuridicos.files.wordpress.com/2013/06/d-str-empw_dvlp-2006-1-01-pdf-s.pdf - http://ensaiosjuridicos.files.wordpress.com/2013/06/d-str-secu-2007-pdf-s.pdf.

[10] Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/research_on_legislation_in_data_privacy_security_and_the_prevention_of_cybercrime_uit.pdf.

[11] Conceito elaborado por Jürgen Habermas.

***Copyrigth* © 2013 - SILVA JR., Nelmon J.** (L. 10753/03 - OPL v.1.0 – FSF/GNU GPL/Key administrated by: CC BY-NC-ND, v.3.0)